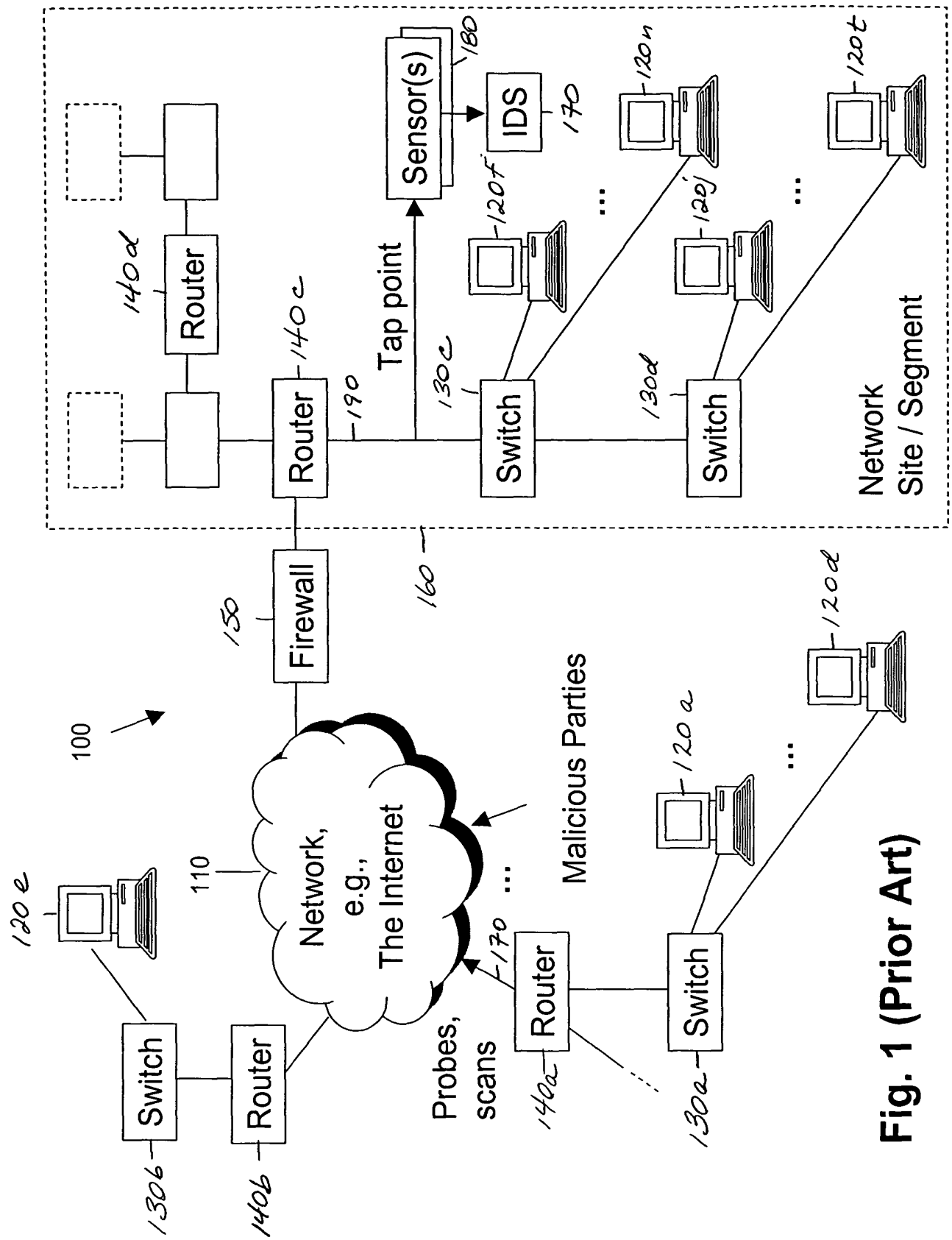

Fig. 1 (Prior Art)

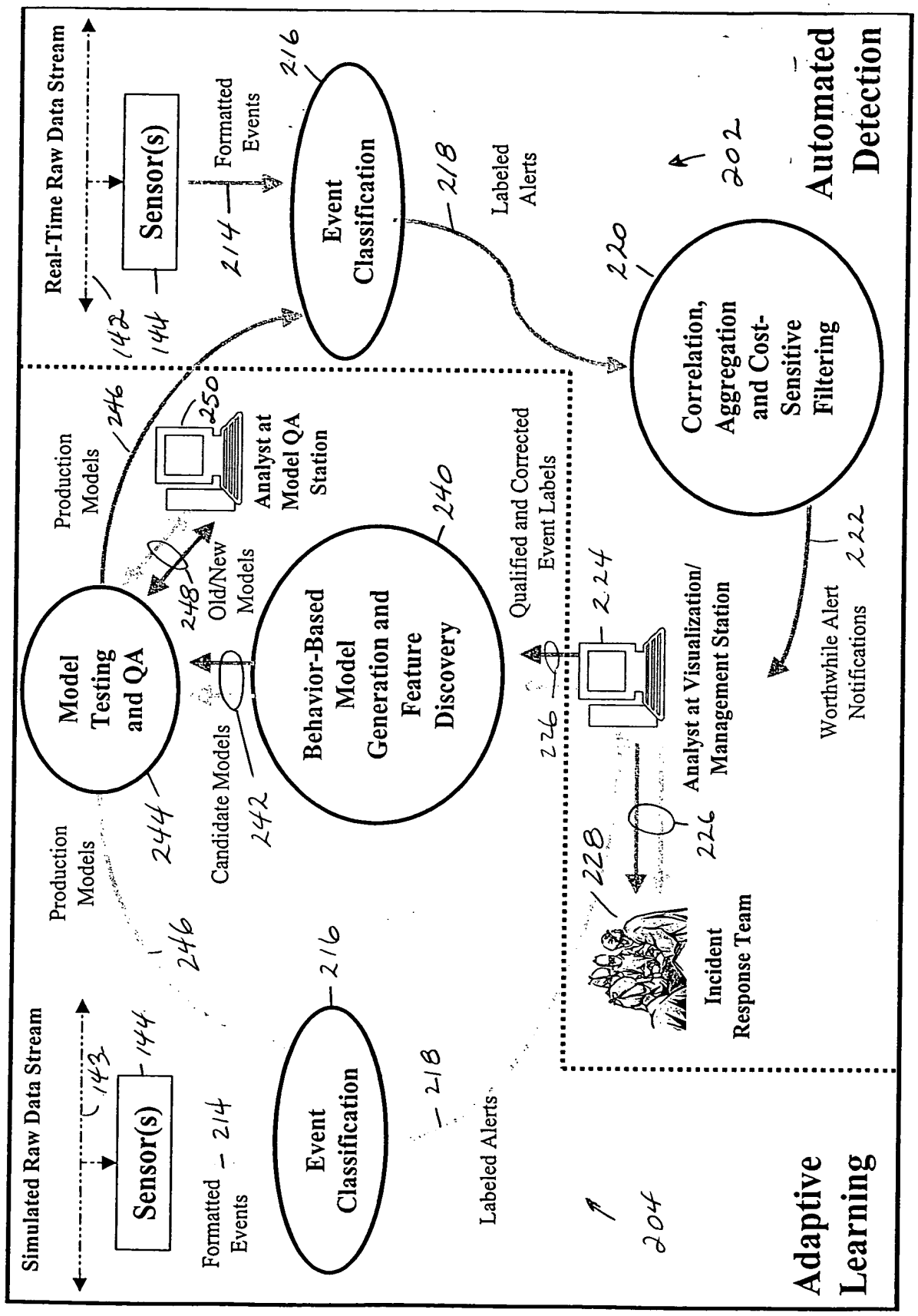
200
Simulated Raw Data Stream
143
Sensor(s)
144
Formatted Events
214
Event Classification
216
Labeled Alerts
218
Production Models
246
Model Testing and QA
244
Candidate Models
242
Old/New Models
248
Analyst at Model QA Station
250
Behavior-Based Model Generation and Feature Discovery
240
Qualified and Corrected Event Labels
226
Analyst at Visualization/ Management Station
224
Incident Response Team
228
Adaptive Learning
204
Real-Time Raw Data Stream
142
Sensor(s)
144
Formatted Events
214
Event Classification
216
Labeled Alerts
218
Correlation, Aggregation and Cost-Sensitive Filtering
220
Worthwhile Alert Notifications
222
Automated Detection
202

Fig. 2

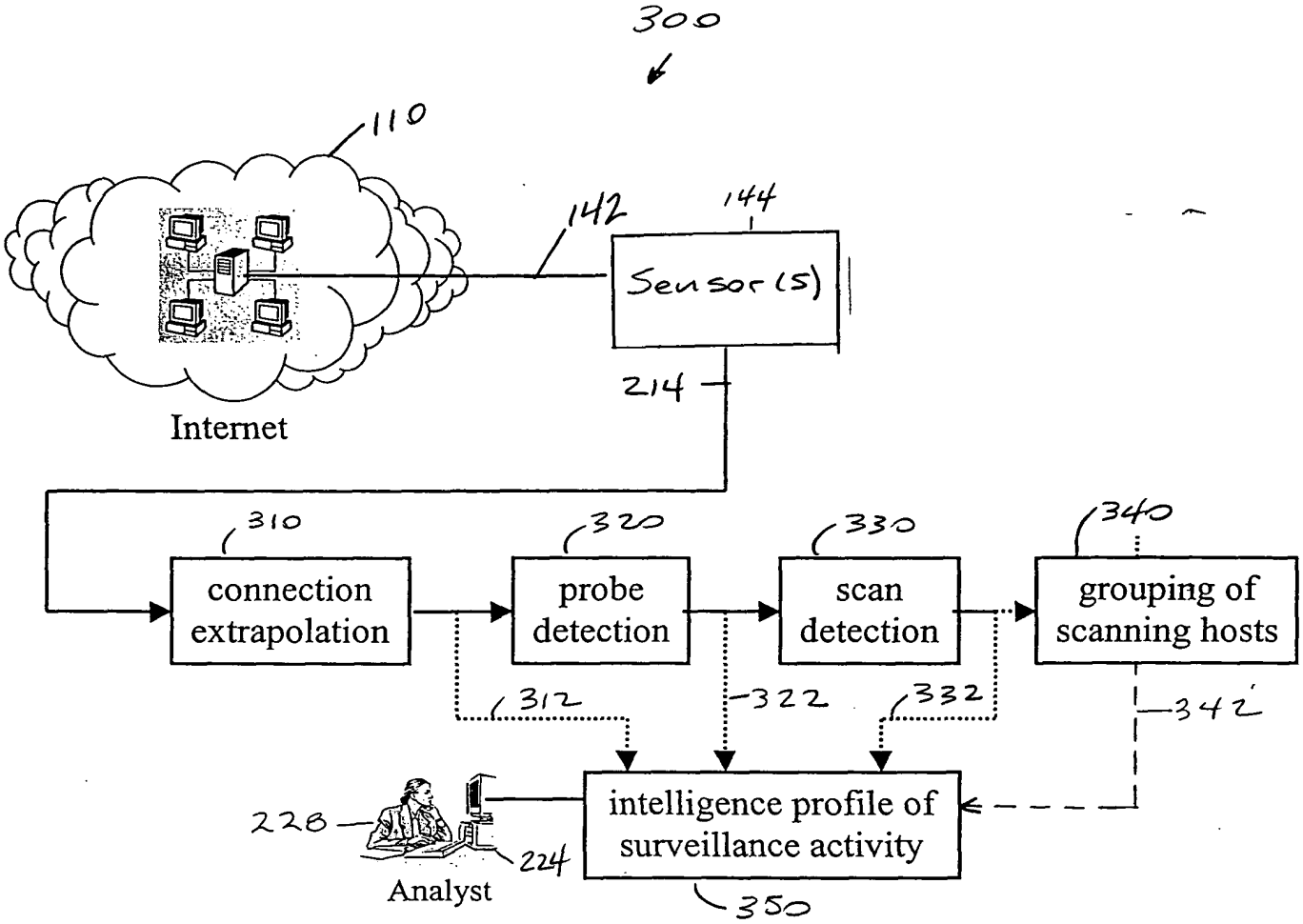
300
110
142
144
Sensor(s)
214
Internet
310
320
330
340
connection extrapolation
probe detection
scan detection
grouping of scanning hosts
312
322
332
342
226
224
Analyst
intelligence profile of surveillance activity
350

Fig. 3

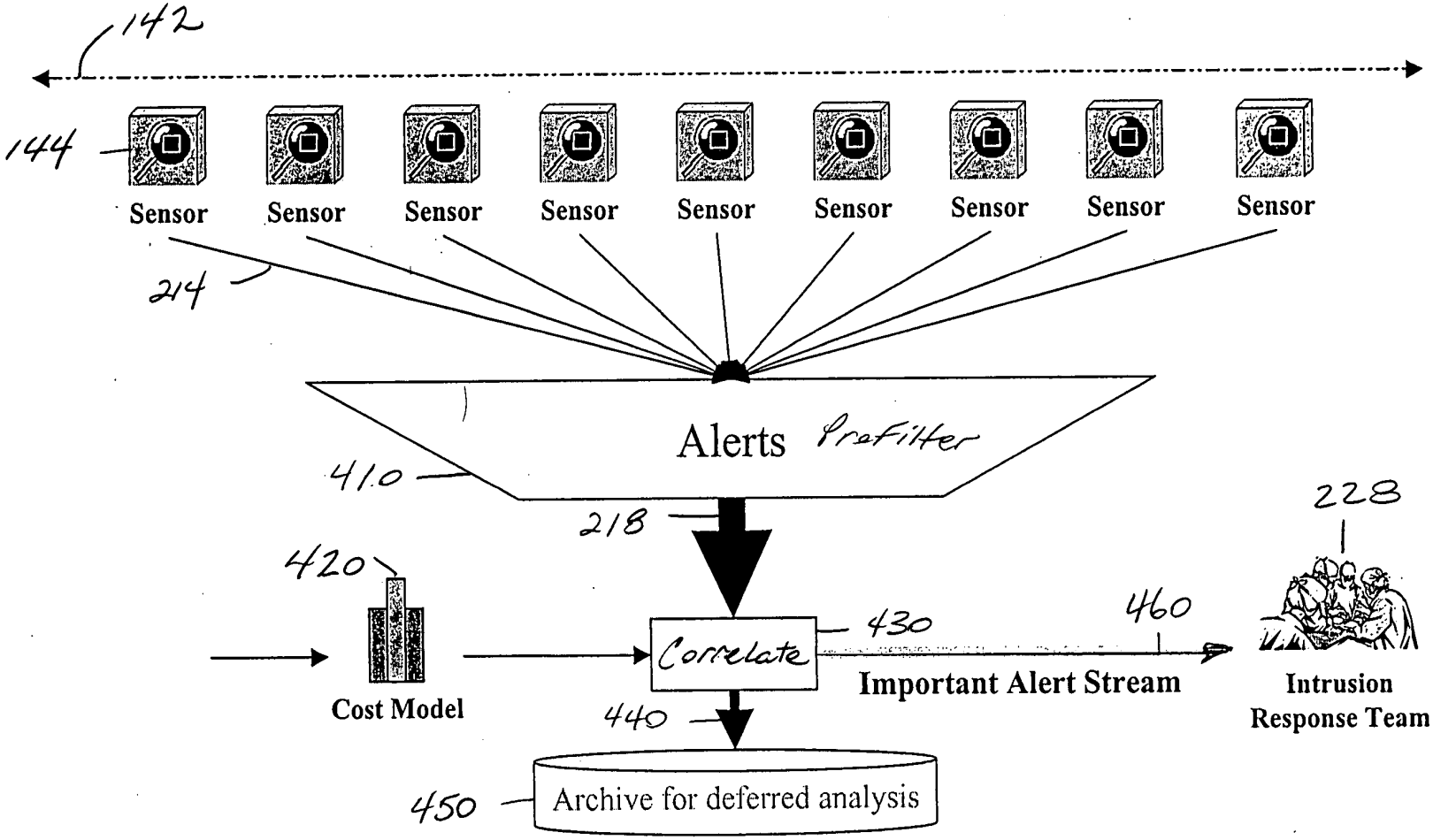
142
144
Sensor
Sensor
Sensor
Sensor
Sensor
Sensor
Sensor
Sensor
Sensor
214
Alerts
Prefilter
410
218
228
420
430
460
Correlate
Cost Model
Important Alert Stream
Intrusion
Response Team
440
450
Archive for deferred analysis

Fig. 4

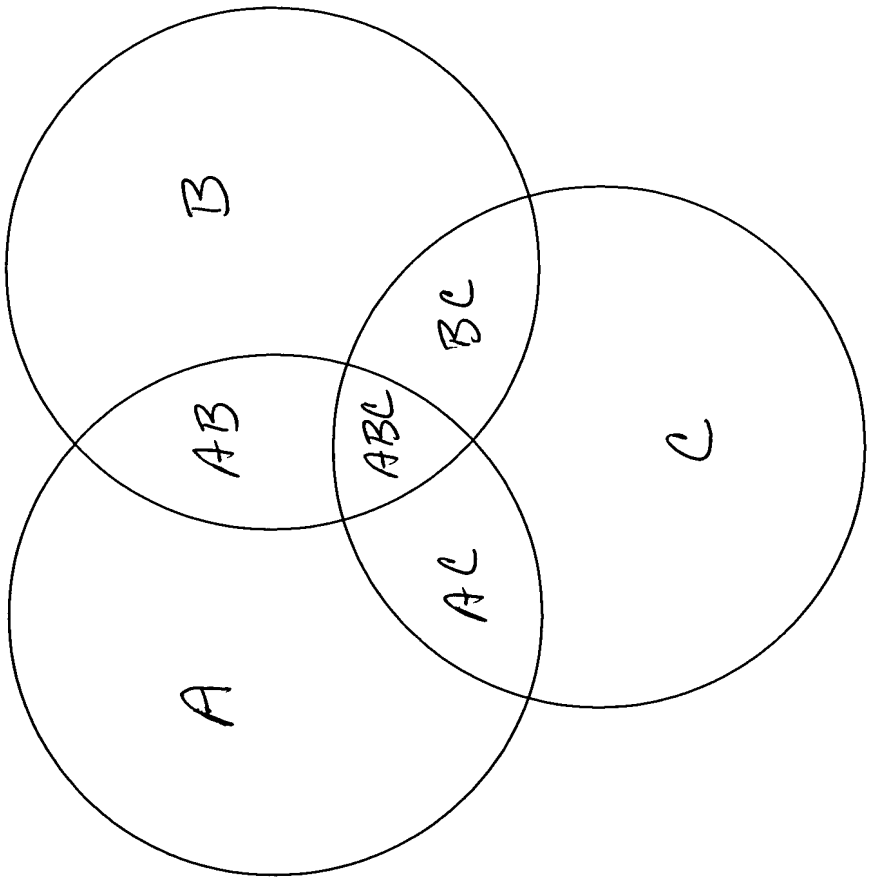

Fig. 5

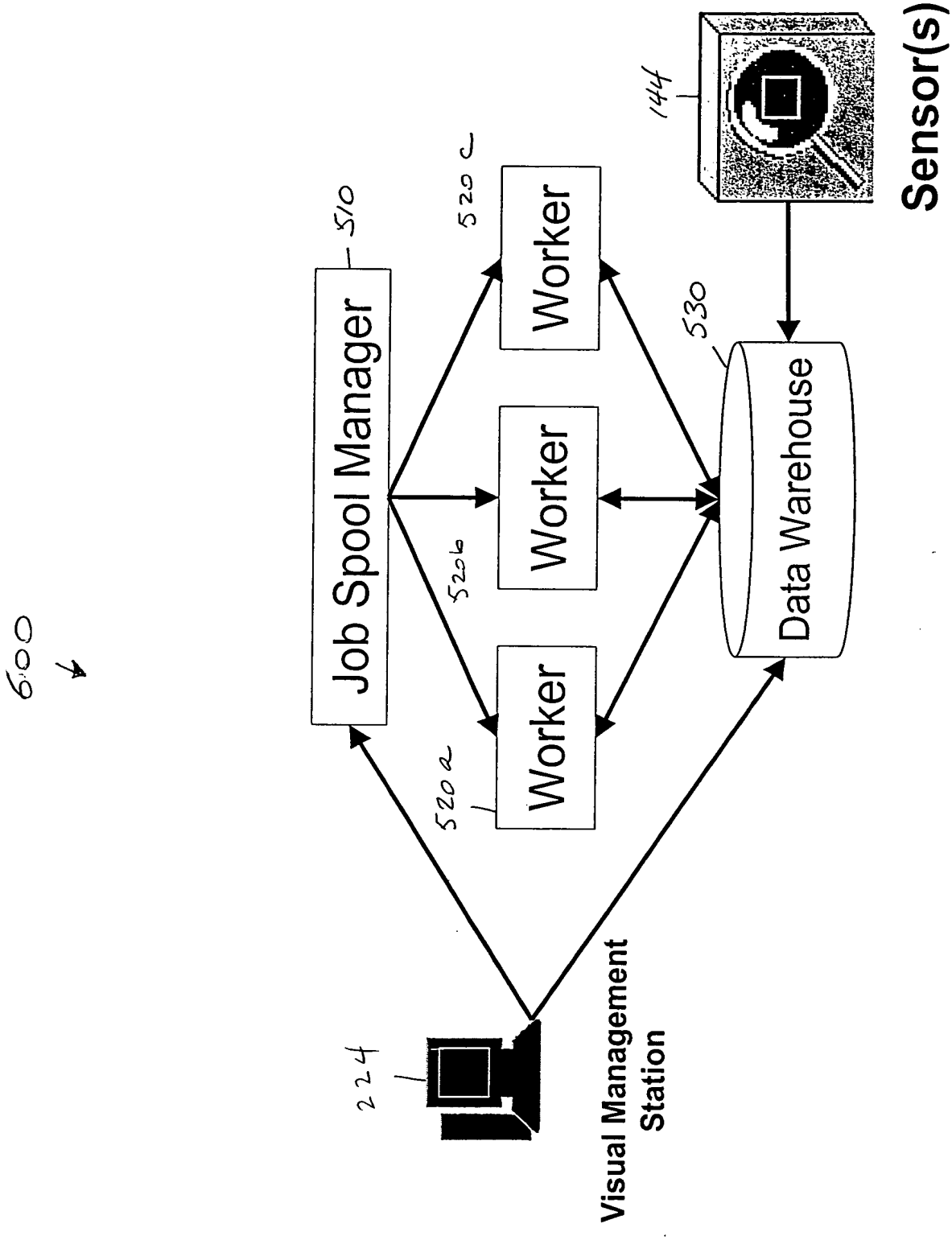
600
Job Spool Manager
510
Worker
520a
Worker
520b
Worker
520c
Data Warehouse
530
Sensor(s)
144
Visual Management Station
224

Fig. 6

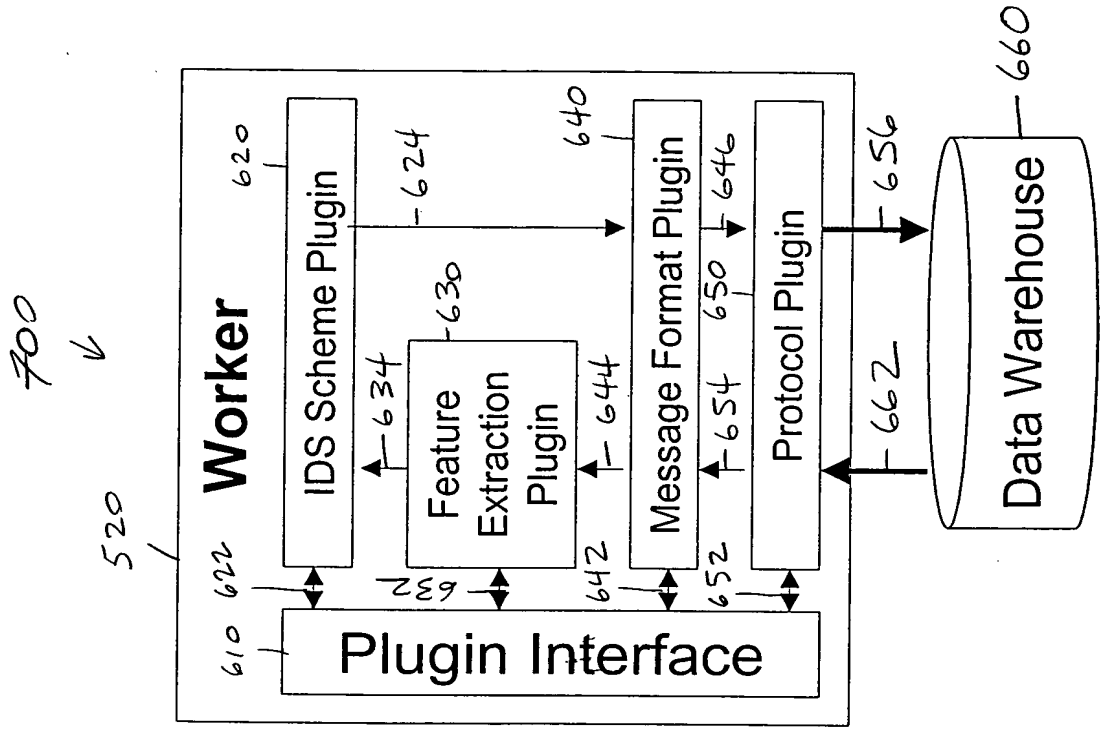
700
520
Worker
620
IDS Scheme Plugin
624
640
Message Format Plugin
646
630
Feature Extraction Plugin
634
644
650
654
Protocol Plugin
656
660
Data Warehouse
662
610
622
632
642
652
Plugin Interface

Fig. 7

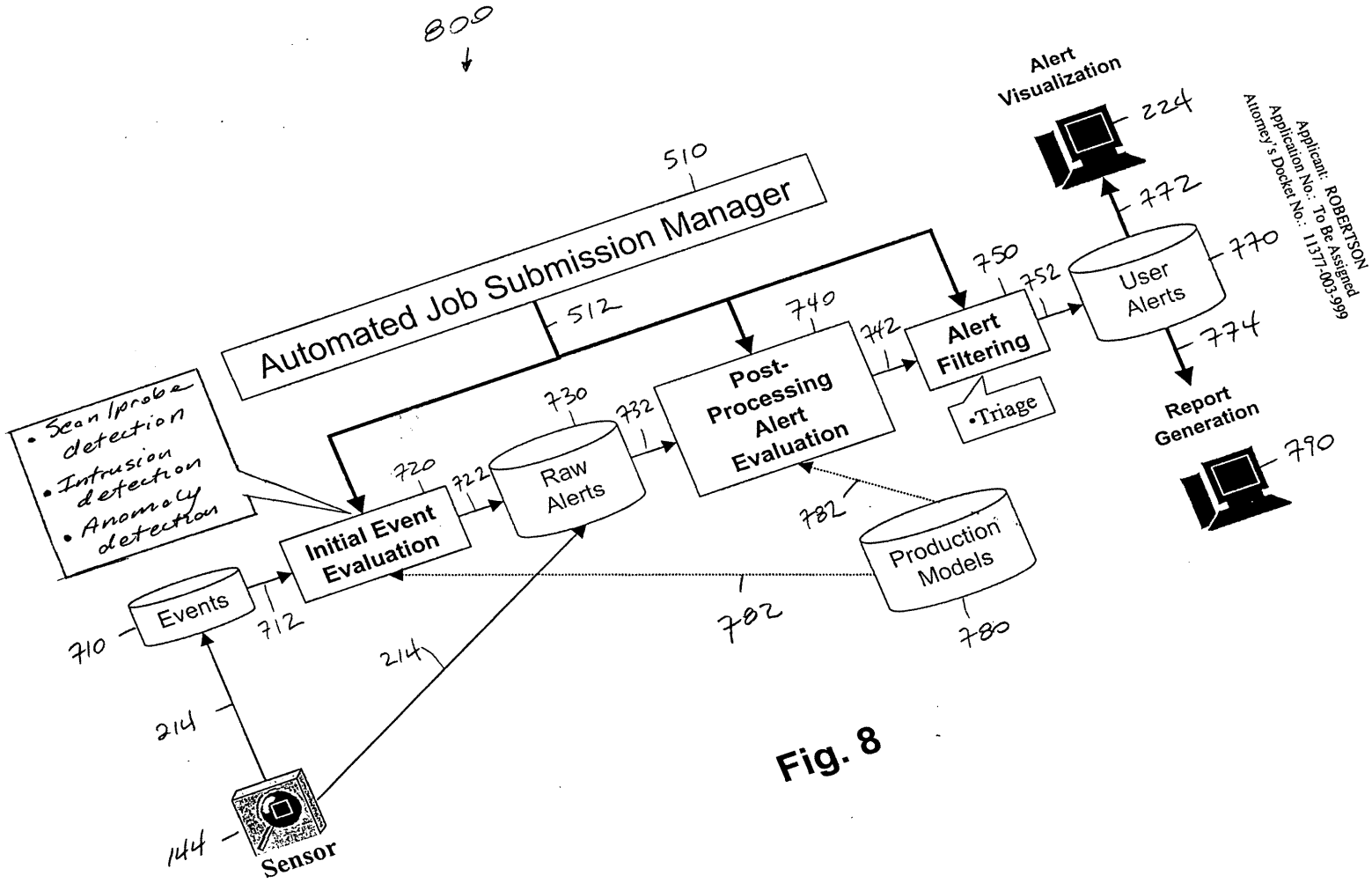
800
Automated Job Submission Manager
510
512
Alert Visualization
224
772
770
User Alerts
750
752
Alert Filtering
740
742
Post-Processing Alert Evaluation
730
732
Raw Alerts
720
722
Initial Event Evaluation
• Scan/probe detection
• Intrusion detection
• Anomaly detection
•Triage
774
Report Generation
790
Production Models
782
780
Events
710
712
214
214
144
Sensor

Fig. 8

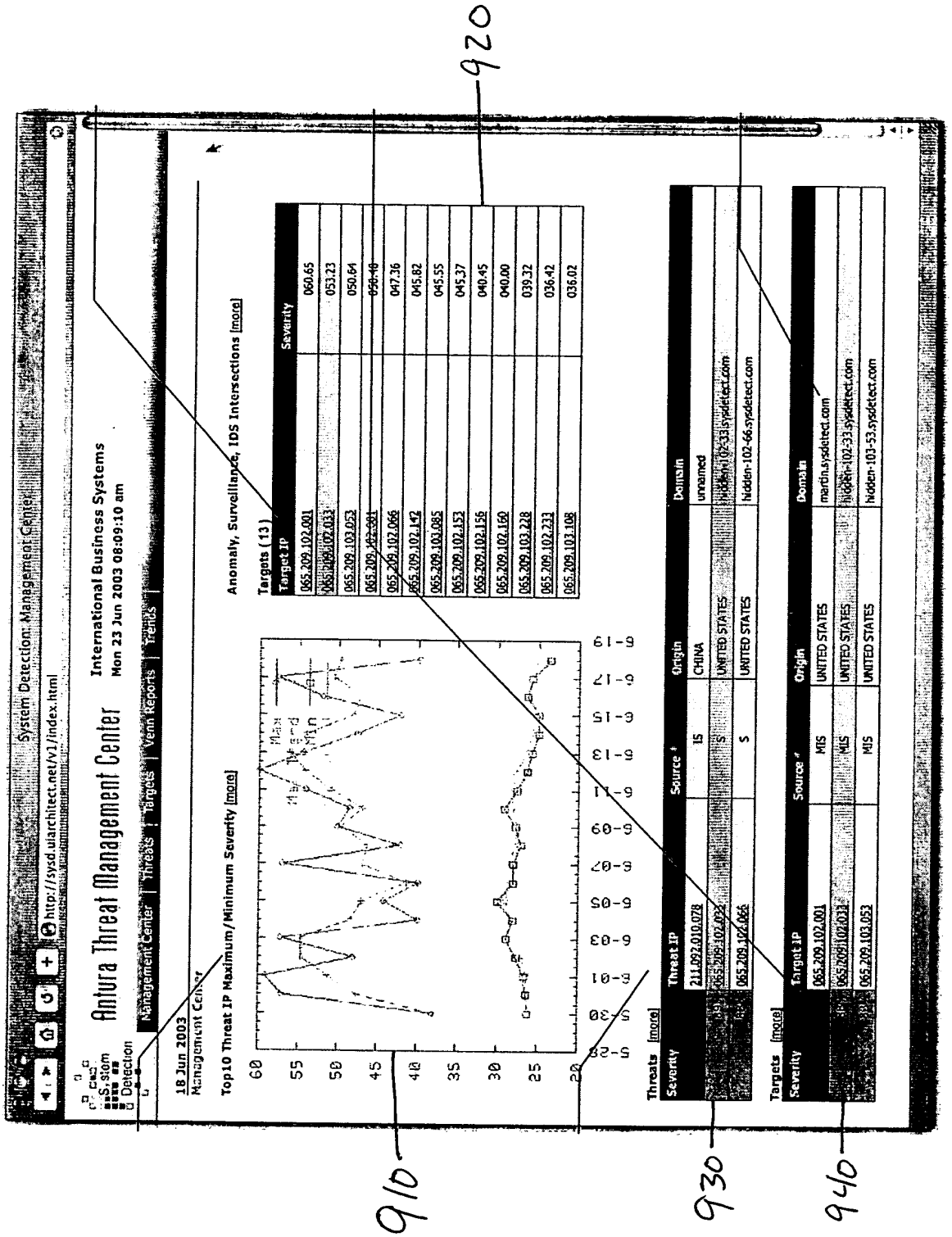
920
910
930
940
System Detection: Management Center
http://sysd.uiarchitect.net/v3/index.html
Antura Threat Management Center
International Business Systems
Mon 23 Jun 2003 08:09:10 am
Management Center | Threats | Targets | Venn Reports | Trends
18 Jun 2003
Management Center
Top10 Threat IP Maximum/Minimum Severity [more]
Anomaly, Surveillance, IDS Intersections [more]
Targets (13)
Target IP
Severity
065.209.102.001
060.65
065.209.102.033
053.23
065.209.103.053
050.64
065.209.102.066
047.36
065.209.102.142
045.82
065.209.103.085
045.55
065.209.102.153
045.37
065.209.102.156
040.45
065.209.102.160
040.00
065.209.103.228
039.32
065.209.102.233
036.42
065.209.103.108
036.02
Threats [more]
Severity
Threat IP
Source #
Origin
Domain
211.092.010.078
IS
CHINA
unnamed
065.209.102.032
S
UNITED STATES
hidden-102-33.sysdetect.com
065.209.102.066
S
UNITED STATES
hidden-102-66.sysdetect.com
Targets [more]
Severity
Target IP
Source #
Origin
Domain
065.209.102.001
MIS
UNITED STATES
marlin.sysdetect.com
065.209.102.033
MIS
UNITED STATES
hidden-102-33.sysdetect.com
065.209.103.053
MIS
UNITED STATES
hidden-103-53.sysdetect.com

Fig. 9

1000

Number of Attackers by Attack Length

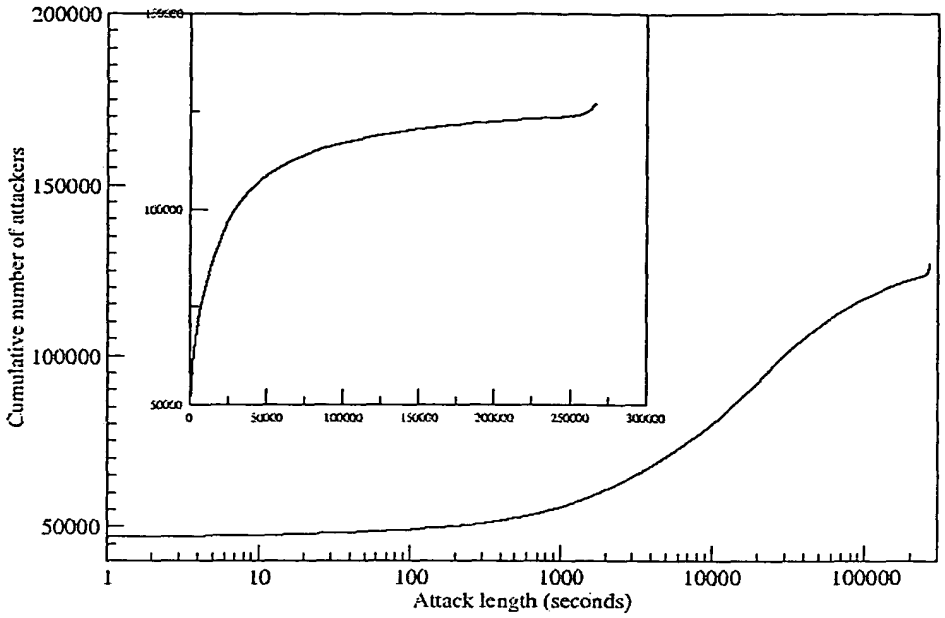

Fig. 10

1100

Number of Attackers by Average Intraprobe Delay

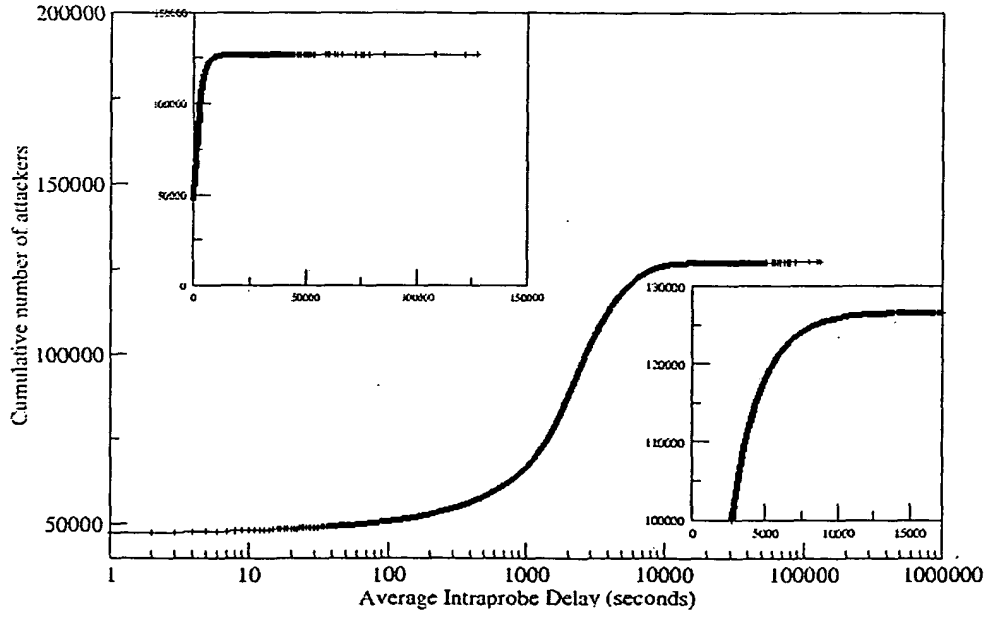

Fig. 11

1200

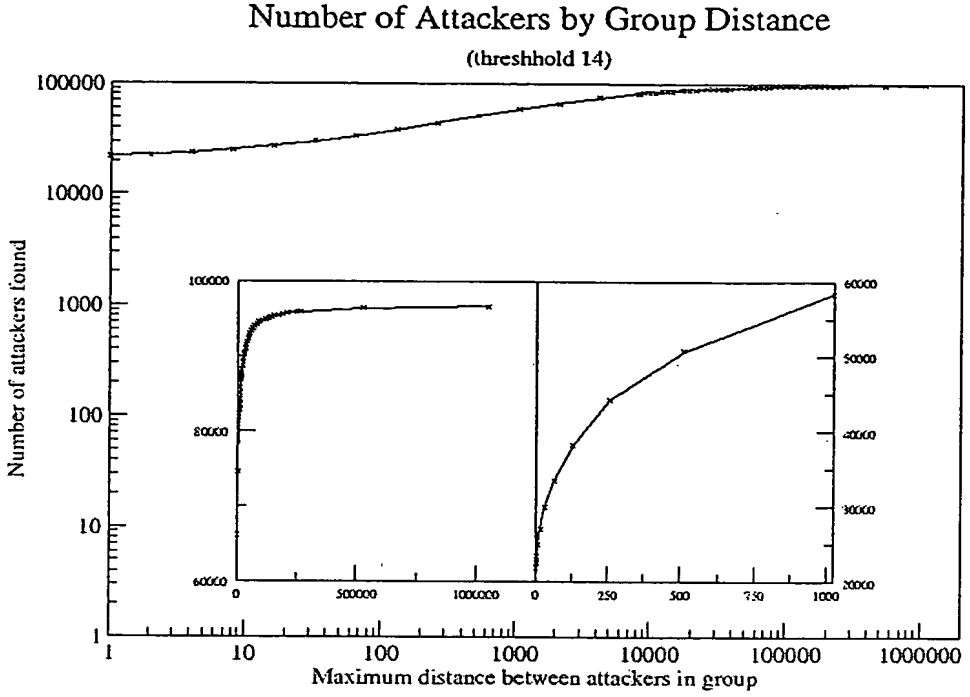

Fig. 12

1300

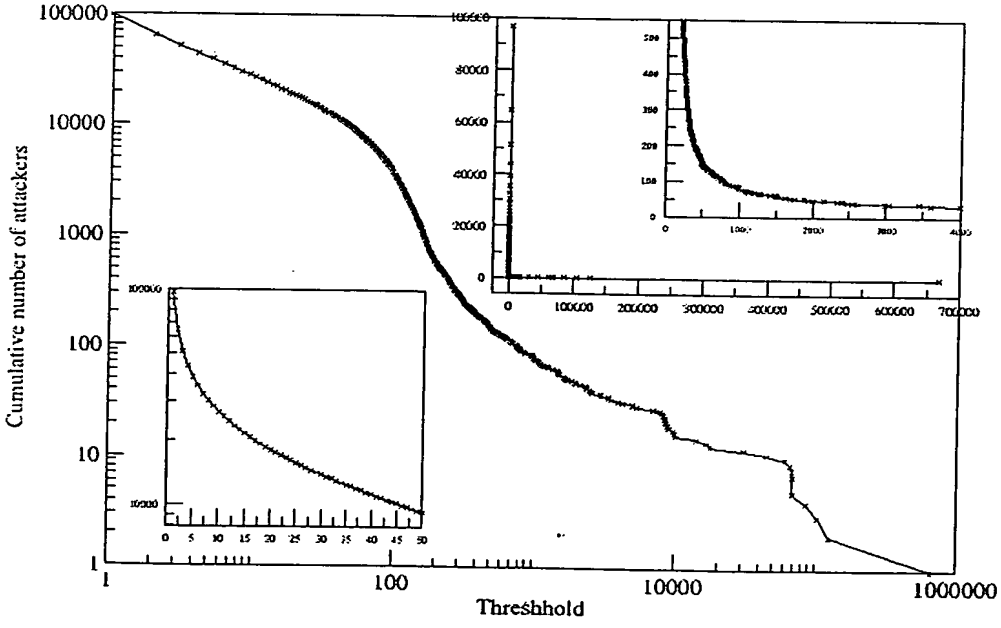

Fig. 13

1400

Distribution of Attacking Hosts

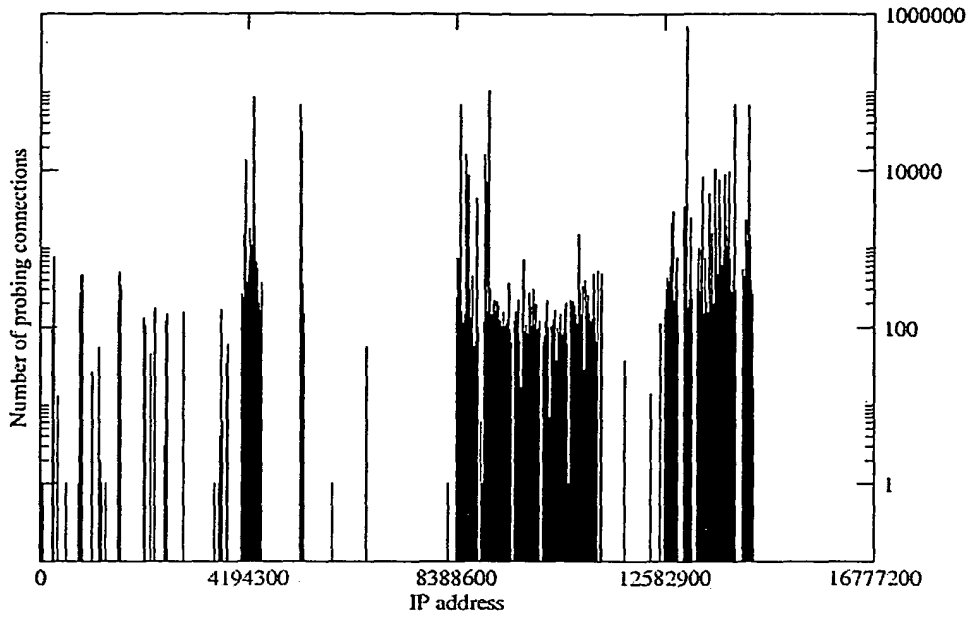

Fig. 14

1500

Distribution of attacked hosts

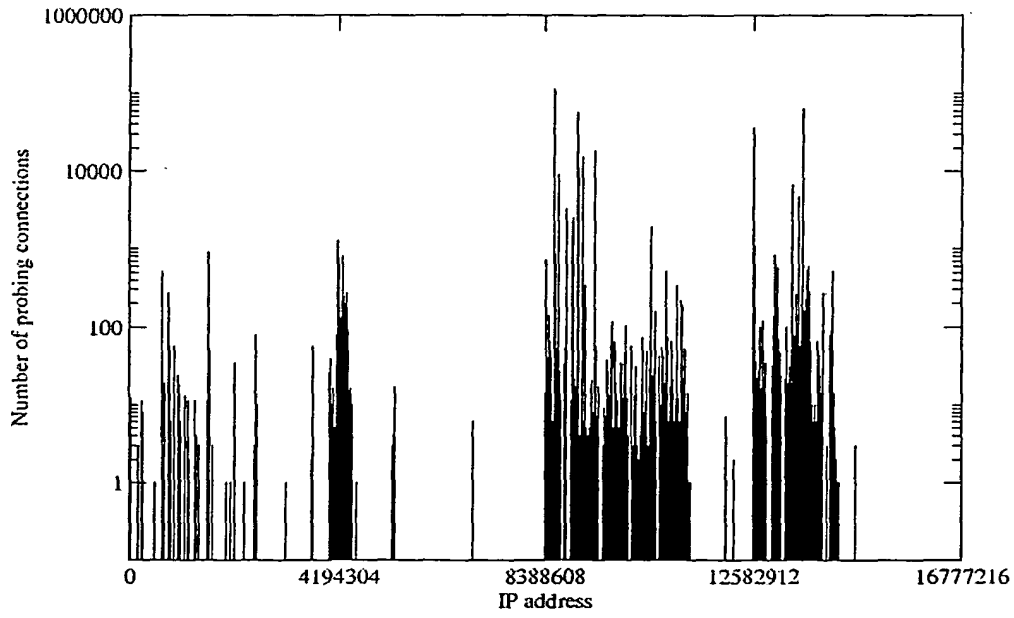

Fig. 15

1600

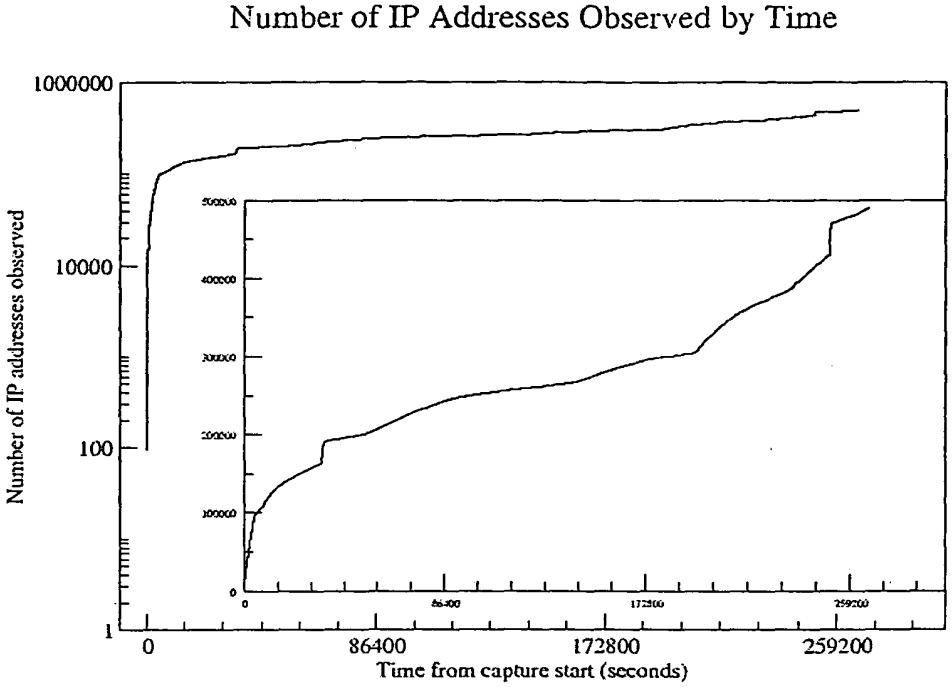
Number of IP Addresses Observed by Time
1000000
10000
100
1
Number of IP addresses observed
0
86400
172800
259200
Time from capture start (seconds)

Fig. 16